EXHIBIT 12

Control access to apps based on user & device context

Allow users to unblock apps with remediation messages in Context Aware Access

Use remediation messages to help users unblock themselves

Next: Use Context-Aware Access with configuration groups

Using remediation messages and custom messages in Context-Aware Access, you can help users unblock themselves when a policy prevents them from accessing an app. These optional (but recommended) messages can help get users back to productivity and reduce support calls for admins.

For example, say that a user on a mobile device is using Gmail in the office successfully during the day, but is blocked when they try to access Gmail at home in the evening. When remediation messages are enabled, they will see guidance on how to address the reason they are blocked.

Remediation and custom messages are supported for access levels created in both Basic mode and Advanced mode. Also, they are supported for both Core Services and SAML apps.

Use remediation messages and custom messages to help your users unblock themselves

When blocked, your users can encounter:

- **Default message**—Displays if you have not added remediation messages or custom messages. An example default message is: **Your organization's policy is blocking access to this app**.
- **Remediation messages**—Replaces the default message. The messages are system generated, and correspond to the specific policy violation that blocked the user.
  Remediation messages can present several remediation options to the user, which they can expand by clicking **Show more options**. In the case of several remediation options, the user needs to complete the steps for any one of the available options to unblock themselves.
- **Custom message**—Adds specific help for the user, such as additional advice on getting unblocked or a helpful link to click. You add custom messages as needed. A custom message can appear in conjunction with the default message, or with remediation messages.

This table shows the interactivity of these messages:

Remediation messages turned on?	Custom message added?	Messages the user sees
No	No	Default message only
Yes	No	Remediation messages only. In some cases the default message might display if the remediation messages can't be generated.
No	Yes	Default message and custom message
Yes	Yes	Remediation messages and custom message

Understand remediation messages

Each remediation action corresponds to an attribute which is causing access to be denied. The following table summarizes possible remediation messages that the user might see. The messages are

created systematically depending on the policy that was violated.

Note that different messages can be shown for the same attribute according to the expectation in the access level. For example, if the access level is *device.screen_lock_enabled == true*, the message is **Set a screen password on your device**. If access level is *device.screen_lock_enabled == false*, the message is **Remove the screen password from your device**. Removing a screen password could be less secure, so the user should confirm this action with the admin.

Actual messages might differ from the messages displayed below.

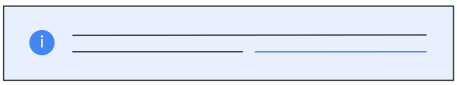
Attribute	Message
Admin approval	Switch to a device approved by your organization. Contact your admin if you don't have access to one.
	Switch to a device that's not associated with your organization. Note, this could be less secure, so you may want to confirm this with your admin.
Company owned device	Switch to a device owned by your organization. Contact your admin if you don't have access to one.
	Switch to a device that's not owned by your organization.
CTS profile match	Reset your device to factory settings.
	Your device can't access this app with an OEM Android installation. Contact your admin for more info.
Encryption	Switch to a device that has one of the following encryption statuses: [status1, status2].
	Switch to a device that doesn't have the following encryption status: [status]
Has potentially harmful apps	Uninstall any apps listed by Google Play Protect as potentially harmful.
	Your device can't access this app with currently installed apps. Contact your admin for more info.
IP address	You can't access this app from your current IP subnetwork. Contact your admin to learn more.
OS type	Switch to a device that uses one of the following: [os1, os2]
	Switch to a device that doesn't use: os1
OS version	Update your device to [OS version X] or higher
	Update your device to an OS version lower than [OS version X]
Partner Attributes	Install [PARTNER NAME] on your device. [1]
	Your device isn't meeting some requirements, based on information from [PARTNER NAME]. [2]
Region code	You can't access this app from your current location. Contact your admin to learn more.
Screen lock	Set a screen password on your device.
	Remove the screen password from your device. Note, this could be less secure, so you may want to confirm this with your admin.
Verify apps	Enable Google Play Protect on your device.
	Disable Google Play Protect on your device.
Verified boot	Follow your device manufacturer's instructions to lock the bootloader.
	Follow your device manufacturer's instructions to unlock the bootloader.
Verified Chrome OS	Install a verified Chrome OS on your device.
	You can't access this app with a verified Chrome OS.

[1] Make sure the partner security app (for example, Lookout) is installed on the device. If it's installed but the user is still seeing this message, the device might not be properly enrolled into the partner MDM. Check the partner dashboard to verify if this is the case. If required, contact the partner to resolve the issue.

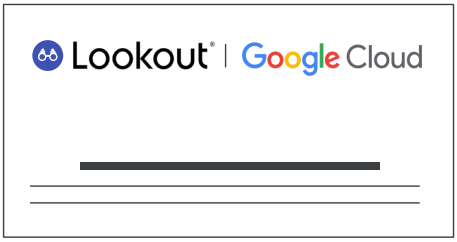
[2] Check the partner app on the device for more details. If required, contact the partner to resolve the issue.

Understand remediation messages and third-party partner integrations

As an administrator, you can integrate supported third-party partners (those that are part of the BeyondCorp Alliance) with Google endpoint management in Google Admin console. This informational text displays in the remediation message interface to explain that partner messages can be available to users:



For example, from Lookout:



For details, go to Set up third-party partner integrations.

Common errors to resolve before remediation or custom messages can be seen by the user

These errors must be cleared before users can view remediation messages:

Your device can't be recognized. There may be different steps depending on your device type.

Google doesn't recognize the login device. The remediation step depends on the platform.

- **Desktop devices**—Users must use a Chrome profile with the Endpoint Verification extension installed. Users can't login to Google Workspace apps through incognito, guest, or personal profiles. Note that this error message can display when a user tries to sign in to a new device for the first time. In that case, the user must sync with the Endpoint Verification extension and refresh the browser.
- **Mobile devices**—For devices to be recognized by CAA, they need to be managed by Google endpoint management (basic or advanced management). For details, go to Manage devices with Google endpoint management. Additionally, devices might need to sync before Google can recognize where the login occurred. For details, see Sync your device.

Sync your device

- **Desktop devices**—Users must sync with the Endpoint Verification extension.
- **Desktop devices**—Devices under advanced management can sync with the device policy app. Devices under basic management can wait for the device to sync automatically, or the user can re-login into any Google app. Let the user know that device sync can take some time.
  - **iOS devices**—Google sessions across different applications are tracked with sessions or tokens in Safari. If the Safari tokens are deleted (manually by the user or Apple ITP), the subsequent logins cannot be mapped to the original logged in device. This can cause the new logins to be blocked with "Your device can't be recognized. There may be different steps depending on your device type" message if remediation is enabled. This issue can occur both on basic and advanced managed devices.

    The user needs to complete the following steps to unblock themselves:

1. Remove the Google enterprise account from all Google applications.
   Log out the Google account from Safari and remove it from any non-Google application which might be using it.
2. Delete Safari cookies and cache .
3. Log into any Google first-party application, such as Drive or Gmail.
4. Access all of the remaining Google first-party applications to verify that you have access.
5. If access to non-Google applications is needed, sign in to the applications within a few days of logging into the Google applications.
   If you do not sign in within 30 days of step 3 and the application is blocked, restart from step 1.

Implement remediation or custom messages

Turn on remediation messages

1. Sign in with an *administrator* account to the **Google Admin console**.
   If you aren't using an administrator account, you can't access the Admin console.
2. From the Admin console Home page, go to **Security** > Access and data control > **Context-Aware Access**.
3. Select **User message.**
4. Under Remediation messages, click **OFF** and slide right to turn the messages **ON**. You'll see a check mark.
5. Click **Save**.
   You can also add a custom message at this point.

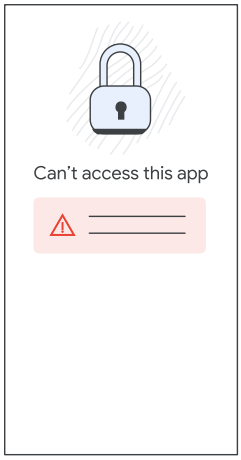
Add a custom message

1. Sign in with an *administrator* account to the **Google Admin console**.
   If you aren't using an administrator account, you can't access the Admin console.
2. From the Admin console Home page, go to **Security** > **Access and data control** > **Context-Aware Access**.
3. Select **User message**.
4. Under Additional custom message, enter your message.
5. Click **Preview** to see what the user will see.
6. Click **Save**.

User experience for remediation and custom messages

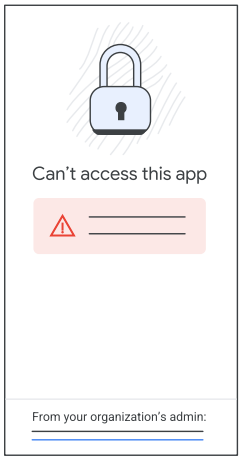
Default message only

This is an example of a message the user sees if no remediation messages or custom message is configured.



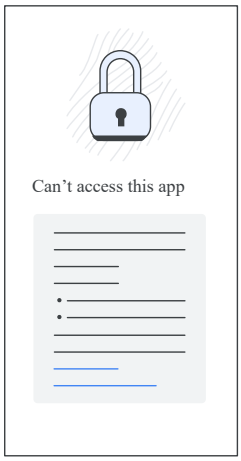
Default message and custom message

This is an example of a message the user sees if no remediation messages are configured, but the custom message is provided.



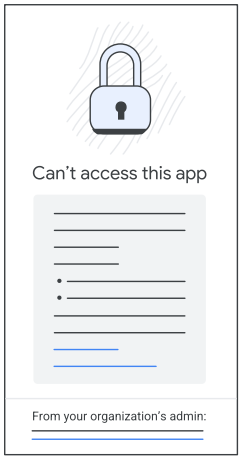
Remediation message only

This is an example of a message the user sees if remediation messages are configured with no custom message. The user clicks **Show more options** to expand the remediation steps.



Remediation and custom message

This is an example of a message the user sees if both remediation messages and the custom message are configured. The user clicks **Show more options** to expand the remediation steps.



Context-Aware Access remediation and custom messages FAQ

Expand all | Collapse all

- Can remediation cause any additional Access Denied cases?
- Why don't the remediation messages reflect the current policies?
- How long does it take for the user to get access after completing the remediation actions?
- Why do Users still see the same remediation options after completing the remediation action?
- Why do remediation message options change without any action on the device?
- Why are remediation messages missing even though they are enabled?
- Do users see the custom user message if remediation is enabled?
- How do I enable remediations for Device policies?
- Why does the **Your device can't be recognized** remediation message display if the Endpoint Verification extension is syncing?

Next: Use Context-Aware Access with configuration groups

Need more help?
Try these next steps:

Post to the help community
Get answers from community members

Ex. 12

Contact us

Tell us more and we'll help you get there

Ex. 12